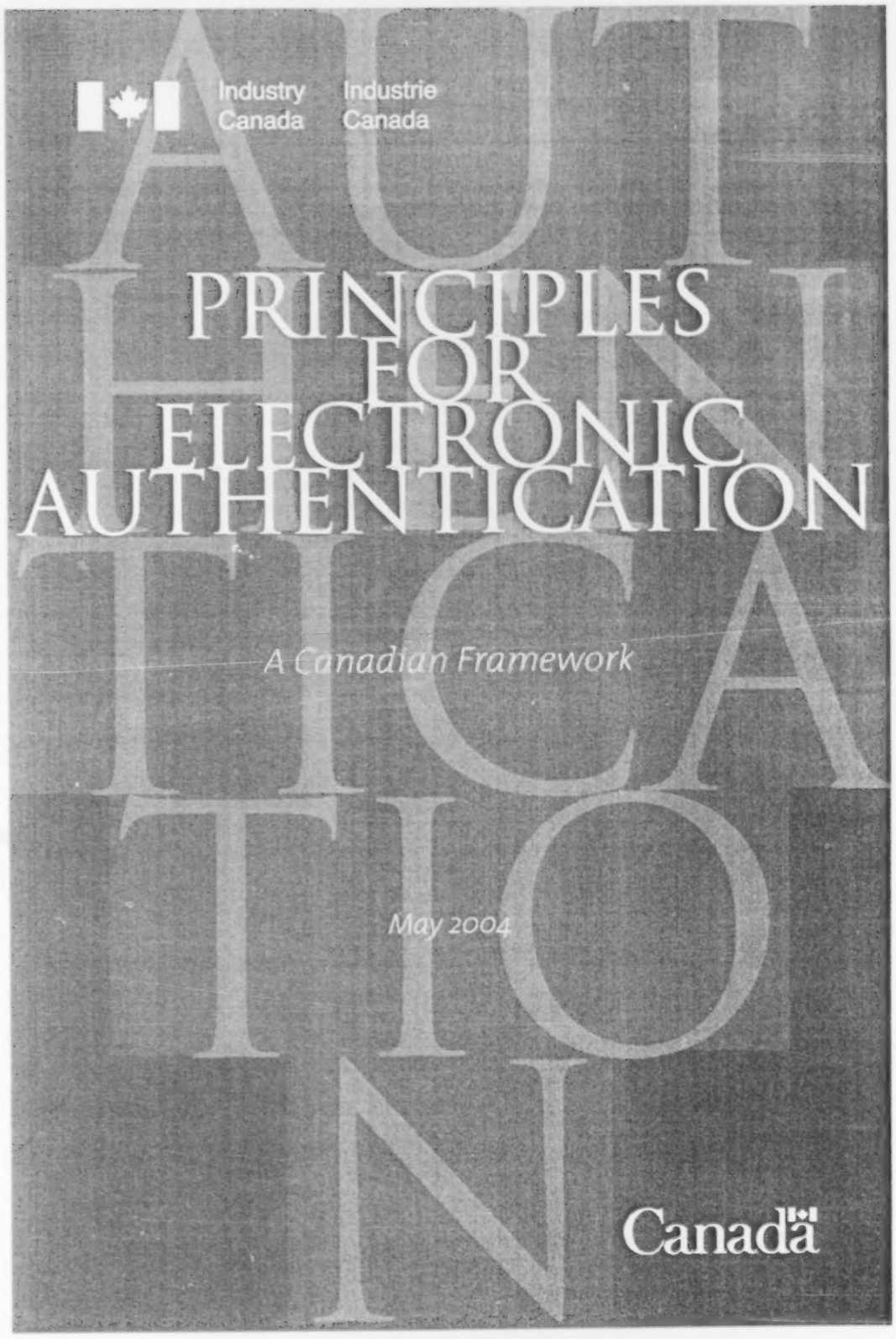

Industry Canada
Industrie Canada
PRINCIPLES FOR ELECTRONIC AUTHENTICATION
A Canadian Framework
May 2004
Canada

This publication is available in multiple formats upon request. Contact the Information Distribution Centre at the numbers listed below.

For additional copies of this publication, please contact:

Information Distribution Centre
Communications and Marketing Branch
Industry Canada
Room 268D, West Tower
235 Queen Street
Ottawa ON K1A 0H5

Tel.: (613) 947-7466
Fax: (613) 954-6436
E-mail: **publications@ic.gc.ca**

This publication, as well as additional background information on the Principles, is also available electronically on the World Wide Web at the following address: **http://strategis.ic.gc.ca/authen**

Permission to Reproduce
Except as otherwise specifically noted, the information in this publication may be reproduced, in part or in whole and by any means, without charge or further permission from Industry Canada, provided that due diligence is exercised in ensuring the accuracy of the information reproduced; that Industry Canada is identified as the source institution; and that the reproduction is not represented as an official version of the information reproduced, nor as having been made in affiliation with, or with the endorsement of, Industry Canada.

For permission to reproduce the information in this publication for commercial redistribution, please e-mail: **copyright.droitdauteur@communication.gc.ca**.

Cat. No. Iu64-16/2004
ISBN 0-662-67949-0
540468

10% recycled material

104-05918/

CONTENTS

Introduction 2

Why and How to Use the Principles 4

About the principles 6

Concepts and Terminology 6

Scope and Nature of the Principles 9

Principles 12

Principle 1: Responsibilities of Participants 12

Principle 2: Risk Management 14

Principle 3: Security 16

Principle 4: Privacy 18

Principle 5: Disclosure Requirements 20

Principle 6: Complaints Handling 22

Additional Information and References 24

INTRODUCTION

All Canadians — individuals, businesses and governments — share an interest in ensuring that electronic communications are secure. As our use of public electronic networks continues to evolve, from searching the Internet for information to exchanging information and money online, we need greater assurance that these messages and transactions are secure and that our privacy is protected. Authentication of electronic communications can make a significant contribution to meeting this need and to building user confidence.

The Principles for Electronic Authentication are designed to function as benchmarks for the development, provision and use of authentication services in Canada. The Principles are intended to form the basis of codes of conduct, voluntary initiatives and guidelines tailored to the requirements of specific industries and government. For individual and business users of authentication services, the Principles are intended to be a useful source of information and benchmarks against which to evaluate services offered in the marketplace.

The Principles were developed by the Authentication Principles Working Group, convened by Industry Canada and with broad representation from industry, professional associations, consumer groups and various levels of government. The following organizations participated in the Working Group and supported the development of the Principles:

Bell Canada

Canadian Advanced Technology Alliance

Canadian Bankers Association

Canadian Bar Association

Canadian Institute of Chartered Accountants

Canadian Payments Association

Certified General Accountants Association of Canada

Deloitte & Touche LLP Canada

Digital Discretion Inc.

Gowling Lafleur Henderson LLP

Industry Canada (Electronic Commerce Branch and Office of Consumer Affairs)

Information Technology Association of Canada

Insurance Bureau of Canada

Juricert Services Inc.

Province of British Columbia

Province of Ontario

Public Interest Advocacy Centre

RBC Financial Group

Retail Council of Canada

Scotiabank

Spyrus Inc.

Standards Council of Canada

Teranet Inc.

Treasury Board of Canada Secretariat

University of Ottawa Law School

Visa Canada Association

WHY AND HOW TO USE THE PRINCIPLES

The Principles are intended to provide guidance for the development, implementation and use of authentication products and services in Canada. They complement the existing governance structure[1] for authentication by establishing benchmarks to ensure that authentication products and services embody sound business and market practices, meet the needs of Canadians and are accepted internationally.

The governance structure that applies to authentication services in Canada today consists of, among other instruments, the Government of Canada's 1998 Cryptography Policy, federal and provincial legislation, including the 2000 *Personal Information Protection and Electronic Documents Act*, the *Principles of Consumer Protection for Electronic Commerce*, developed in 2001, and the *Canadian Code of Practice for Consumer Protection in Electronic Commerce* (January 2004).

It is anticipated that the Principles for Electronic Authentication will be of greatest use to those involved in the design, development and deployment of authentication services and products. The Principles identify the functions and responsibilities of participants in authentication processes and provide a framework to assess and manage the risks that accompany these responsibilities. The Principles also identify security, privacy, disclosure and complaint-handling matters that need to be taken into account at each stage of the design, development, implementation and assessment of an authentication process.

Those involved with the design, implementation and ongoing operation of authentication processes are encouraged not only to respect the Principles but also to publicize them. The Principles should form the basis of codes of conduct, voluntary initiatives and guidelines that are tailored to the

1 The term *governance structure* refers to the range of policy tools, regulatory instruments and self-regulatory guidelines that relate to the development and implementation of authentication services in Canada.

requirements of specific industries and government. Such initiatives are strongly encouraged, and can provide strategic advantages in domestic and international markets.

The Principles are intended as a useful source of information and as benchmarks for individual and business users of authentication. While the Principles define the responsibilities of participants (Principle 1) and address aspects of risk management (Principle 2), they do not address the liabilities that could be borne by the various participants involved in authentication processes. In particular, the Principles do not address issues of consumer protection or liability, and should not be interpreted as allocating liability to end users of authentication services. Legislative or other measures may evolve to address the needs of end users, particularly the risk and liability assumed by consumers participating in authentication processes.

The authentication environment is dynamic and the technologies used will continue to evolve. Although every effort has been made to define principles that can encompass foreseeable developments, they are open to revision as needed to take into account significant technological advances, changes in market characteristics and international developments. Comments and views on the Principles are welcome at any time and should be addressed to:

Richard Simpson
Director General
Electronic Commerce Branch
Industry Canada
300 Slater Street, Room D2090
Ottawa ON K1A 0C8

Comments can also be provided by facsimile at (613) 941-0178 or by electronic mail at **authen@ic.gc.ca**.

The Principles will be reviewed at least every five years, or more frequently if necessary. The Authentication Principles Working Group is charged with the periodic review and revision of the Principles. The composition of this group will be assessed and adjusted as appropriate as the authentication environment evolves.

ABOUT THE PRINCIPLES

CONCEPTS AND TERMINOLOGY

The subject of the Principles is the authentication of electronic communications in its broadest sense. Therefore, the concepts and terms used in this document relate to all participants, actions and techniques comprising all aspects of authentication, whether considered from the technical, legal or business perspective. Each concept or term relates to the others, none should be considered in isolation.

Functions

For the purposes of the Principles, the authentication process is viewed as encompassing six functions. Their relative importance depends on the purpose and structure of the authentication process.

AUTHENTICATION ADMINISTRATION. Administering the measure or measures designed to confirm the attributes of a participant and those designed to support the credibility of a participant's claim to possess those attributes and thereby be authenticated.

SPECIFICATION. Establishing or selecting an authentication process and delivery mechanism.

END USE. Originating or receiving an authenticated electronic communication and relying on the authentication of the attributes.

STANDARDS DEVELOPMENT. Establishing standards that support the continued development of processes designed to facilitate authentication of electronic communications.

COMPLIANCE ASSESSMENT. Observing and making informed evaluations of the practices associated with authentication to ensure that appropriate policies, procedures and standards are being followed.

INFRASTRUCTURE PROVISION. Providing the capability that enables authentication, including functions to authenticate identity or the integrity of electronic communications.

Definitions

The Authentication Principles Working Group considered existing definitions, particularly those created by international standards groups such as the International Organization for Standardization (ISO), when developing the Principles. However, the broad scope of the Principles resulted in definitions that may not correspond to similar terms used by specific communities.[2]

AUTHENTICATION. A process that attests to the attributes of participants in an electronic communication or to the integrity of the communication.

ATTRIBUTES. Information concerning the identity, privileges or rights of a participant or other authenticated entity.

PARTICIPANT. An individual or organization participating in an authentication process, whether directly or through another authenticated entity, such as a data service or object, hardware device or software program.

ELECTRONIC COMMUNICATION. An electronic transmission, message or transaction.

INTEGRITY. Assurance that the information in an electronic communication has not been modified or corrupted during the process of communication.

Authentication is intended to promote trust in electronic communication. Participants in an electronic communication are provided with assurance that other participants have been authenticated using technological methods, and that those other participants, as well as the integrity of the communication itself, can be trusted to the degree specified by the authenticator (the designated authority that confirms the attributes of a participant or entity and then attests to them to other participants in the electronic communication).

2 For example, the definition of *authentication* encompasses "message authentication," which is commonly understood to refer to processes applied to ensure message integrity. Furthermore, a term that is not defined or used in connection with the Principles is *non-repudiation*. The term is commonly used to describe a technical standard to be met by an authentication process. However, the term is misleading in a more general context because it incorrectly implies a conclusion of law.

Participants rely on the authentication of an electronic communication to the extent that they can assess the reliability of the authentication. The technological methods and specifications used for authentication are often based on cryptographic techniques.

The act of authentication depends on some prior activity that authorizes participants, based on their presentation of certain specified attributes, to enter into an authenticated electronic communication. A participant's attributes may relate to a person's identity. As an alternative, the required attributes may identify the person's rights or privileges to enter into the electronic communication. In the latter case, a participant may not need to be identified personally to other participants.

Authentication processes frequently attest to the attributes of non-human entities. For example, an organization participating in an authentication process may choose to authenticate a server. In this case, the server's attributes may relate to the privileges it has been assigned to communicate with other servers or clients on the system.

Authorization is the responsibility of a designated authority. Many models are available for carrying out such authorization. For example, a simple exchange of information may require as authorization only the presentation of user identification and a password. An electronic system established to communicate highly confidential and private information may, by contrast, require in-person presentation of two or more pieces of reliable identification combined with unique personal characteristics, such as fingerprints. Yet another model designates an employer as the authority, who then authorizes a group of employees to engage in electronic communications on its behalf on the basis of individuals' job functions.

SCOPE AND NATURE OF THE PRINCIPLES

These Principles relate to the authentication of electronic communications in its broadest sense.

The Principles are intended to apply to authentication processes used in connection with electronic communications that take place between businesses or governments and other organizations, between organizations and individuals (consumers or citizens), and between individuals.

A range of relationships can exist between authenticators and end users, and among end users. Many of these relationships are governed by agreements. The Principles are intended to guide the development of these agreements and to apply to the full range of these relationships.

Parties to negotiated contracts are usually best able to determine which terms and conditions suit their particular needs. However, in situations in which a party may not have the opportunity to negotiate the terms of their interaction with the other party (or parties) to the transaction, the Principles are of particular importance.

The Principles should be considered and applied as a unified whole.

The provisions in the various Principles are interrelated and interdependent; they cannot achieve their purposes if they are implemented selectively, although not all Principles may apply in all cases. Those applying the Principles to define or implement authentication processes are encouraged to exceed the benchmarks that the Principles establish and to expand upon them to address the requirements of their particular security environment or application.

The Principles are expressed at a high level of generality and technological neutrality.

Canadians can choose from a variety of technologies to authenticate their electronic communications, according to the nature of the particular communication and the requirements of the participants.

The implementation of authentication processes also differs, depending on the business or legal objectives to be met, as well as the characteristics of the environment in which the electronic communication takes place, such as security and privacy needs and other legislative or regulatory obligations. These factors define the functionality required of an authentication process and, in some cases, even the type of authentication used.

The Principles are designed to foster a well-functioning, fair and competitive marketplace for authentication products and services.

Authentication processes should be effective, efficient, reliable and easy-to-use, and should respect the interests of individuals and organizations. Whenever possible, the Principles accommodate choice of technology, services and solutions, choice of the degree of reliance by end users, and choice of tools used to ensure compliance.

The Principles emphasize proportionality.

The degree of responsibility and risk that each participant in the authentication process assumes should be in proportion to the degree of knowledge and control that the participant can reasonably be expected to have and to exercise, as well as to the nature and value of the

electronic communication itself. Since participants can perform multiple functions in varying combinations, the degree of responsibility and risk assumed by any one participant may vary, depending on these functions.

The Principles emphasize data privacy.

The Principles recognize the existing and evolving legal framework for the protection of the privacy of personal information in Canada, and address how privacy protection standards apply to authentication. The Principles address the intersection of privacy-respecting and security-enhancing practices. The importance of privacy to Canadians requires those who design and implement authentication measures to consider how their systems can best respect privacy at every stage of the process.

The Principles have been developed to ensure compatibility with international developments in authentication.

Canada is committed to continued involvement in various international fora addressing the need for global frameworks for authentication. This participation ensures that Canada's approach is in step with that of other jurisdictions, enabling Canadian industry to be competitive in the international marketplace.

PRINCIPLES

PRINCIPLE 1: RESPONSIBILITIES OF PARTICIPANTS

Participants in an authentication process should be aware of the functions they are performing and of the responsibilities associated with those functions. Participants' responsibilities are proportional to the degree of knowledge and control they can reasonably be expected to have and to exercise.

All participants should act prudently and take reasonable steps to inform themselves of the nature of the authentication process, including its requirements and limitations, to protect information associated with the process, and to manage the risks to which they are exposed (see Principle 2).

Participants' specific responsibilities depend on the function or functions they carry out, as follows.

Authentication Administration

The administrator is responsible for following appropriate and trusted measures so that other participants may have confidence in the credibility of claimed attributes. When any part of the administration function is delegated to a third party, the administrator is responsible for ensuring that the third party also follows appropriate and trusted processes.

Specification

The specifying participant is responsible for choosing a system, such as an authentication infrastructure or process, that meets the privacy, security and other policy and legal requirements associated with an electronic communication. This may include the mechanism by which a participant's authority to enter into the electronic communication, and the integrity of the communication itself, can be ascertained.

End Use

The responsibility of end users to inform themselves about the authentication process is limited by the extent of clear and conspicuous information disclosed to them (see Principle 5). The responsibility of end users to protect information relating to the authentication process may be limited by legal or contractual obligations. Such obligations may

require disclosure of information concerning the process they use to determine the reliability of electronic communications.

Standards Development

Standards developers are responsible for ensuring that standards are robust, scalable and adaptive to encourage uniformity in authentication implementations. This responsibility extends to incorporating a wide range of views and best practices into proposed standards to ensure they are relevant, up-to-date and continuously applicable. Responsible standards development takes into account both existing and emerging technologies and international practices.

Compliance Assessment

Those who assess compliance are responsible for maintaining and applying a professional and up-to-date level of knowledge and practice so they can provide a reasoned and informed evaluation of authentication processes.

Infrastructure Provision

Infrastructure providers are responsible for following best practices and standards to implement and support the infrastructure that enables authentication.

PRINCIPLE 2:
RISK MANAGEMENT

The risks associated with authentication processes for electronic communications should be identified, assessed and managed in a reasonable, fair and efficient manner.

The responsibilities of participants concerning risk management are proportional to the degree of knowledge and control that each participant can reasonably be expected to have and to exercise. It is recognized that the ability of participants to identify, assess and manage risk varies substantially, and that some types of participants (e.g. consumers and small enterprises) cannot reasonably be expected to identify, assess and manage risk to the same extent as participants that have access to more significant resources or who define the working relationships.

Identification

Risks should be identified to the extent possible. Risks may be financial — including immediate, direct and consequential damages arising from faulty execution or delay in execution of the communication — or may relate to, among other things, loss of confidentiality or privacy, damages to reputation, or identity theft.

Assessment

The seriousness and potential impact of risks should be assessed. When assessing risk, special attention should be paid to the circumstances under which the authentication process is relied upon. When evaluating and assessing risk, it can be helpful to take into account the responsibilities associated with each of the six functions (see Principle 1).

Management

Risks should be managed to the point of greatest economic efficiency by being assumed, avoided, re-allocated or mitigated. Risk is economically efficient when the residual risk that a participant bears after prudently managing risk does not outweigh the benefits gained from participating.

Role of Contracts

Contracts may be used to provide a framework for each participant's involvement. Contracts should be clear about the risks that each party is assuming and should allocate risk in a reasonable, fair and efficient manner. For contracts that are not freely negotiated among equal parties,[3] efforts may be needed to protect the interests of weaker parties.[4]

Decision Making

Regardless of the means used to allocate risk, the resulting allocation should be reasonable and fair and take into account the ability of participants to manage risk or absorb losses. It should also create incentives for those developing and implementing authentication processes to ensure that their products and services are secure and reliable.

---

3 An example of this is a contract that imposes terms of service on users.

4 Such efforts can be made at the industry sector level through the inclusion of provisions in codes, or at the government level through policy or legislation.

PRINCIPLE 3: SECURITY

All participants in an authentication process should be responsible and accountable for security, in proportion to their roles in that process. All participants have a responsibility to contribute to the mitigation of risk through sound security practices. However, infrastructure providers and those involved in authentication administration bear much of the burden to design and maintain systems based on policies and procedures that take into consideration legislation, regulation, policy, industry standards and the socio-cultural environment.[5]

The purpose of information security is to mitigate the risks inherent in the electronic sharing of information. Infrastructure providers and those involved in the specification and administration of authentication processes often take the initiative when designing and implementing security mechanisms, and therefore have an interest in raising awareness by informing other participants about these mechanisms and participants' role in their maintenance (for example, selecting and safeguarding user passwords). Security mechanisms should conform to generally accepted standards.

Protection, Detection and Response

As appropriate, all participants should be made aware and, at all times, be conscious of security risks, known threats and vulnerabilities, and available safeguards. In an authentication process, a security incident that affects a single participant may have implications for all participants. Participants should therefore act at all times to prevent such incidents, and should be ready and able to respond appropriately. Information about known threats, vulnerabilities and risks should be shared among participants, as appropriate, as an effective preventive measure, to enhance vigilance in

5 This principle accepts and adopts the Organisation for Economic Co-operation and Development's (OECD) *OECD Guidelines for the Security of Information Systems and Networks* (see page 24). The complete text of the Guidelines is available online at **www.oecd.org/dataoecd/16/22/15582260.pdf**

detection and to ensure timely response. Effective information security measures should be proportional to the information risk and should respect the rights of participants, in keeping with the democratic principles of an open society.

Information technology evolves rapidly. It is therefore sound security management to ensure that all participants are reliably informed of new and existing threats, and of the role participants are expected to play in the prevention and detection of and response to security incidents.

Review and Assessment

The continual review and assessment of security programs is essential to ensure the ongoing efficacy of a security program. Those who establish authentication processes, and infrastructure providers in particular, in concert with the other participants in the authentication process, should verify and demonstrate their adherence to sound security management practices, each in proportion to the role they play. A person independent of the authentication process should conduct a periodic review of the security practices associated with the process. Such a review should be integral to accreditation and certification against generally accepted standards.

PRINCIPLE 4: PRIVACY

Organizations engaged in the design or operation of authentication processes should comply with the data protection standards set out in relevant codes of practice (privacy codes) in addition to complying with applicable legislation and jurisprudence (privacy laws).[6] In particular, the collection, use and disclosure of personal information[7] in the context of authentication should be minimized.

Identity-based authentication can conflict with privacy considerations. For example, stronger authentication may require the collection and comparison of more personal information. However, minimizing the collection, use and disclosure of personal information in the authentication context is fundamental for security as well as privacy reasons. Privacy safeguards can actually contribute to the security of authentication processes.

Authentication Administration

Authentication administration should involve the collection of personal information only when necessary. Any personal information collected should be used for no purpose other than authentication. Authentication of a business should focus on business attributes rather than personal attributes of individual employees.

---

6 General legislation governing data protection in the private sector that is currently in force includes the federal *Personal Information Protection and Electronic Documents Act* and privacy laws enacted in Alberta, British Columbia and Quebec. Other provinces and territories may choose to enact general data protection legislation. Federal, provincial and territorial privacy legislation that covers the public sector and sector-specific legislation protecting personal information may also apply.

The Canadian Standards Association's *Model Code for the Protection of Personal Information* (CAN/CSA-Q830-96) has been incorporated into the federal *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c 5, as Schedule 1 to that Act. The Code was developed by a multistakeholder working group and adopted by the Standards Council of Canada as a national standard in 1996. Many industry codes of practice also address data protection.

7 As defined in the *Personal Information Protection and Electronic Documents Act*: "any information about an identifiable individual."

If collection of personal information is required, such collection should be minimized. Any use or disclosure of personal information should also be minimized. Personal information should be collected, used or disclosed only with the informed consent of the individual.

Personal information should be retained only for the purpose of authentication.

Specification and Infrastructure Provision

Authentication processes should be designed to require that the least possible amount of personal information be collected, used and disclosed. Process design should take into account the access rights of participants and the obligation of organizations to make information available about their privacy policies. Organizations using authentication processes designed by others have a responsibility to ensure that those processes respect privacy.

End Use

End users of authentication processes and services should take reasonable measures to ensure that personal information within their control is protected from unauthorized collection, use or disclosure.

Standards Development

Authentication standards should be developed in full accordance with the privacy principles set out in privacy laws and codes. Privacy protection should explicitly be built into authentication standards. Standards developers should consider the coincidence of measures that contribute to protection of data privacy with those designed to ensure security of authentication processes.

Compliance Assessment

Compliance assessment should include assessment of whether and how the organization in question is complying with the privacy principles set out in privacy laws and codes. Compliance assessors should protect the confidentiality of personal information they deal with in the context of their assessments, in accordance with privacy laws and codes.

PRINCIPLE 5: DISCLOSURE REQUIREMENTS

Participants that offer authentication services should disclose information to the other participants to ensure that all participants are aware of the risks and the responsibilities associated with participation.

The information that is disclosed about authentication services should include policies, practices and procedures, as well as information about whether the services are periodically reviewed or audited. Appropriate disclosure requires the information to be provided in sufficient detail for the purpose, be in plain language and be conspicuous. All three factors will have a bearing on the knowledge other participants can reasonably be expected to have of the disclosed information.

Extent and Nature of Disclosure

Disclosure should *not* include security-related information that, if disclosed, would introduce vulnerabilities and increase risk. However, the amount and nature of information disclosed should be sufficient for participants to understand their responsibilities and to make informed risk-management decisions concerning reliance on the authentication. The extent and nature of the information may vary depending on whether the end user is an individual or an organization.

Notification

Participants should be notified of the availability of information and of any changes to the information. Evidence of receipt of notification may be required, depending on the nature of the authentication process and associated applications.

Relationship to Other Principles

Participants that offer authentication services should disclose their policy and practices concerning the collection of personal information. Principle 4 more fully addresses personal information and its disclosure. Disclosure requirements should also be considered in conjunction with Principle 1 (Responsibilities of Participants) and Principle 2 (Risk Management).

PRINCIPLE 6: COMPLAINTS HANDLING

Organizations implementing authentication processes should make available a complaints-handling process that enables participants to resolve complaints efficiently and effectively and to respond appropriately to non-compliance issues.

Complaints-handling processes should reflect the following.

Visibility

Information about how and where to direct complaints should be well publicized to all participants and their personnel and to other interested parties, and should include full information about the complaints-handling process.

Accessibility

The complaints-handling process should be easily accessible to all participants, and the organization should ensure that information is readily available on the details of resolving disputes. The process and supporting information should be easy for individuals with complaints to understand and use, be in plain language and be available in the languages in which the products and services were originally offered.

Responsiveness

Complaints should be dealt with promptly and thoroughly. Complaints should be assessed from a security perspective and resolved in priority, according to their potential negative impact on the participants involved or on the authentication implementation as a whole.

Fairness and Objectivity

Each complaint should be addressed in a balanced manner through the complaints-handling process, which should be fair to the complainant and the participant against whom the complaint is made.

Charges

Access to the complaints-handling process should be free-of-charge to the complainant.

Confidentiality and Privacy

Personal information concerning complainants should be available only where needed within the organization handling the complaint and must be actively protected from disclosure, unless the complainant expressly consents to its disclosure.

Accountability

Organizations should ensure that there is an identified individual or identifiable unit responsible for the systematic recording of complaints and outcomes, and for reporting on the actions and decisions of the organization with respect to complaints handling.

Continual Improvement

Continual improvement of the quality of authentication products and services is facilitated through the complaints-handling process, based on customer and other feedback. The complaints-handling process itself should be monitored on an ongoing basis, and reviewed and assessed in light of feedback.

Unresolved Complaints

When complaints cannot be resolved internally, organizations should be willing to use appropriate third-party dispute resolution processes upon request of the complainant, including those administered by private third parties. However, complainants should continue to have access to the justice system.

ADDITIONAL INFORMATION AND REFERENCES

ADDITIONAL INFORMATION

OECD Guidelines for the Security of Information Systems and Networks

1. Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

2. Responsibility

All participants are responsible for the security of information systems and networks.

3. Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

4. Ethics

Participants should respect the legitimate interests of others.

5. Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

6. Risk Assessment

Participants should conduct risk assessments.

7. Security Design and Implementation

Participants should incorporate security as an essential element of information systems and networks.

8. Security Management

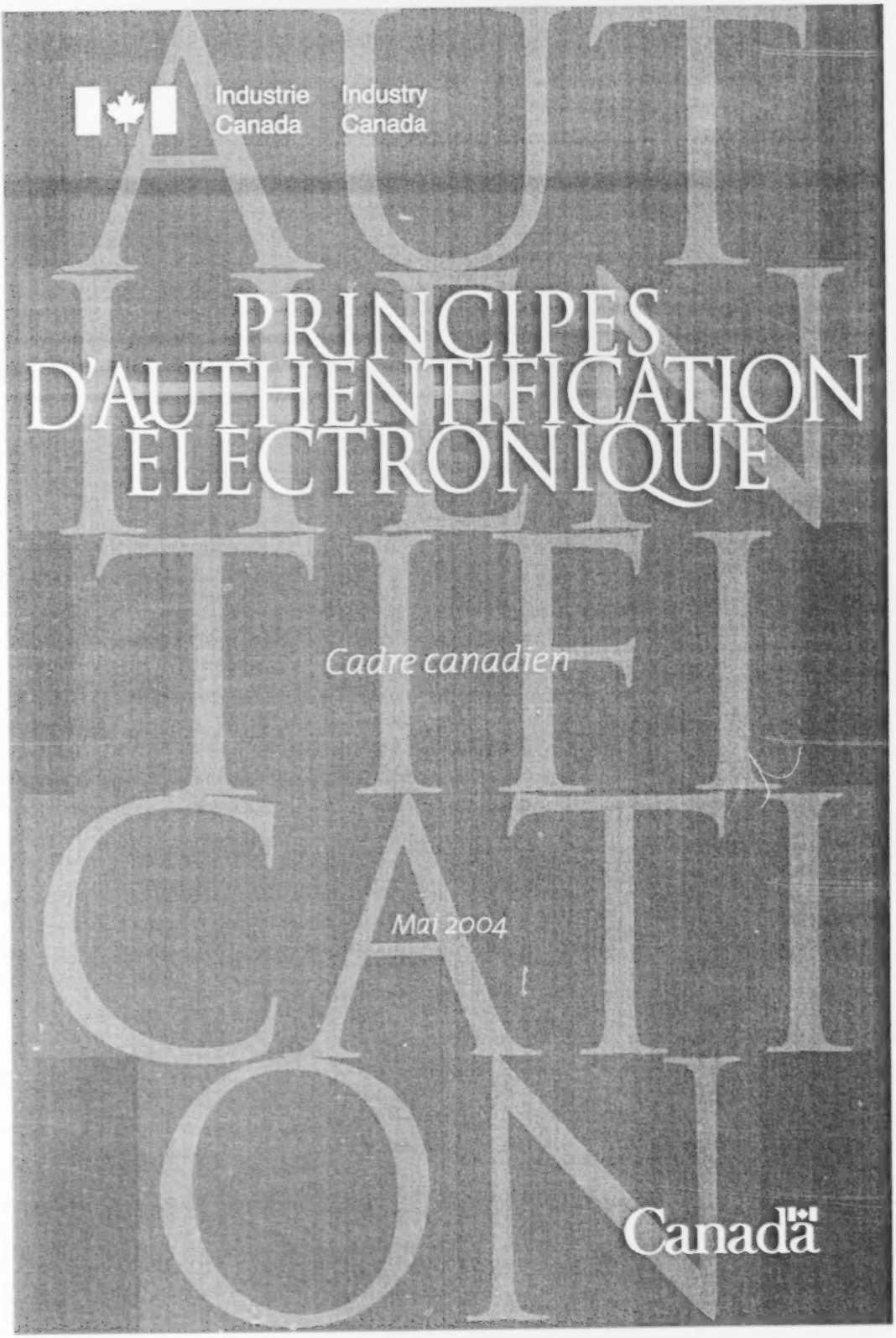
Participants should adopt a comprehensive approach to security management.

9. Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

REFERENCES

See **http://strategis.ic.gc.ca/authen** for a list of general references, as well as a list of domestic and international references and source documents specific to each Principle.


Industrie Canada
Industry Canada
PRINCIPES D'AUTHENTIFICATION ÉLECTRONIQUE
Cadre canadien
Mai 2004
Canada

On peut obtenir cette publication sur supports multiples, sur demande. Communiquer avec le Centre de diffusion de l'information dont les coordonnées suivent.

Pour obtenir des exemplaires supplémentaires de la présente publication, s'adresser au :

Centre de diffusion de l'information
Direction générale des communications et du marketing
Industrie Canada
Bureau 268D, tour Ouest
235, rue Queen
Ottawa (Ontario) K1A 0H5

Téléphone : (613) 947-7466
Télécopieur : (613) 954-6436
Courriel : **publications@ic.gc.ca**

Cette publication ainsi que des renseignements supplémentaires concernant les principes sont offerts par voie électronique sur le Web (**http://strategis.ic.gc.ca/authen-fr**).

Autorisation de reproduction
À moins d'indication contraire, l'information contenue dans cette publication peut être reproduite, en tout ou en partie et par quelque moyen que ce soit, sans frais et sans autre permission d'Industrie Canada, pourvu qu'une diligence raisonnable soit exercée afin d'assurer l'exactitude de l'information reproduite, qu'Industrie Canada soit mentionné comme organisme source et que la reproduction ne soit présentée ni comme une version officielle ni comme une copie ayant été faite en collaboration avec Industrie Canada ou avec son consentement.

Pour obtenir l'autorisation de reproduire l'information contenue dans cette publication à des fins commerciales, faire parvenir un courriel à **copyright.droitdauteur@communication.gc.ca**.

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

N° de catalogue Iu64-16/2004
ISBN 0-662-67949-0
540468

Contient
10 p. 100 de
matières recyclées

TABLE DES MATIÈRES

In••• • • •••• • ____ 2

Pourquoi et comment utiliser les principes 4

Au suje•• ••• ••• ••• •• ____ 6

Concepts et terminologie 6

Portée et nature des principes 9

P••• ••• •• ____ 12

Principe 1 : Responsabilités des parties prenantes 12

Principe 2 : Gestion du risque 14

Principe 3 : Sécurité 16

Principe 4 : Protection des renseignements personnels 18

Principe 5 : Obligations d'information 20

Principe 6 : Traitement des plaintes 22

Informations supplémentaires et références ____ 24

INTRODUCTION

Les parties prenantes canadiennes — les personnes physiques, les entreprises et les administrations publiques — partagent un intérêt commun : faire en sorte que les communications électroniques soient sûres. Étant donné que notre utilisation des réseaux électroniques publics continue d'évoluer, passant d'une simple recherche d'information sur Internet à l'échange d'information et d'argent en ligne, nous avons besoin d'une plus grande assurance que ces messages et ces transactions sont sûrs et que nos renseignements personnels sont protégés. L'authentification des communications électroniques peut faire beaucoup pour répondre à ce besoin et pour instaurer la confiance chez les utilisateurs.

Les présents principes d'authentification électronique sont conçus pour servir de points de repère à l'élaboration, à la prestation et à l'utilisation des services d'authentification au Canada. Les principes sont censés former la base des codes de conduite, des initiatives bénévoles et des lignes directrices adaptés aux exigences d'industries spécifiques et du gouvernement. Pour les personnes physiques et les entreprises qui utilisent les services d'authentification, les principes sont censés constituer une source d'information utile ainsi que des points de repère au regard duquels elles peuvent évaluer les services offerts sur le marché.

Les principes ont été élaborés par le Groupe de travail sur les principes d'authentification qui a été convoqué par Industrie Canada et qui est formé de personnes provenant généralement de l'industrie, d'associations professionnelles, de groupes de consommateurs et de divers niveaux de gouvernement. Les organisations suivantes ont participé au groupe de travail et aidé à l'élaboration des principes :

Alliance canadienne de technologie de pointe

Association canadienne de la technologie de l'information

Association canadienne des paiements

Association des banquiers canadiens

Association des comptables généraux accrédités du Canada

Association du Barreau canadien

Bell Canada

Bureau d'assurance du Canada

Centre pour la défense de l'intérêt public

Conseil canadien des normes

Conseil canadien du commerce de détail

Deloitte & Touche LLP Canada

Digital Discretion Inc.

École de droit de l'Université d'Ottawa

Gowling Lafleur Henderson LLP

Groupe financier RBC

Industrie Canada (Direction générale sur le commerce électronique et Bureau de la consommation)

Institut Canadien des Comptables Agréés

Juricert Services Inc.

Province de l'Ontario

Province de la Colombie-Britannique

Scotiabank

Secrétariat du Conseil du Trésor du Canada

Spyrus Inc.

Teranet Inc.

Visa Canada Association

POURQUOI ET COMMENT UTILISER LES PRINCIPES

Les principes visent à orienter l'élaboration, la mise en œuvre et l'utilisation des produits et des services d'authentification au Canada. Ils sont complémentaires de la structure de gouvernance[1] existante pour l'authentification, car ils établissent des points de repère qui font en sorte que les produits et les services d'authentification incorporent de saines pratiques commerciales, répondent aux besoins des Canadiens et sont acceptés à l'échelle internationale.

La structure de gouvernance qui s'applique aujourd'hui aux services d'authentification au Canada est constituée entre autres, de la Politique du Canada en matière de cryptographie de 1998, de lois fédérales et provinciales, y compris la *Loi sur la protection des renseignements personnels et les documents électroniques* de 2000, les *Principes régissant la protection des consommateurs dans le commerce électronique*, qui ont été élaborés en 2001, et le *Code canadien de pratiques pour la protection des consommateurs dans le commerce électronique* (janvier 2004).

Les principes d'authentification électronique devraient être surtout utiles aux intervenants qui participent à la conception, à l'élaboration et au déploiement des services et des produits d'authentification. Les principes établissent les fonctions et les responsabilités des parties prenantes aux processus d'authentification et ils fournissent un cadre d'évaluation et de gestion des risques liés à ces responsabilités. Les principes font aussi état des questions de sécurité, de protection des renseignements personnels, de divulgation et de traitement des plaintes dont il faut tenir compte à chaque étape de la conception, de l'élaboration, de la mise en œuvre et de l'évaluation d'un processus d'authentification.

Les intervenants qui participent à la conception, à la mise en œuvre et à l'exécution courante des processus d'authentification sont encouragés non seulement à respecter les principes, mais aussi à les faire connaître. Les principes devraient constituer la base des codes de conduite, des initiatives volontaires et des lignes directrices qui

1 L'expression « structure de gouvernance » désigne la gamme d'outils stratégiques, d'instruments réglementaires et de directives d'autoréglementation qui ont trait à l'élaboration et à la mise en œuvre des services d'authentification au Canada.

sont adaptés aux exigences du gouvernement et des secteurs industriels. On encourage fortement de telles initiatives, car elles peuvent offrir des avantages stratégiques sur les marchés nationaux et internationaux.

Les principes sont censés être une source d'information utile et servir de points de repère aux personnes physiques et aux entreprises qui utilisent l'authentification. Bien que les principes définissent les responsabilités des parties prenantes (principe 1) et traitent d'aspects de la gestion du risque (principe 2), ils n'abordent pas la question des obligations qui pourraient incomber aux diverses parties qui participent au processus d'authentification, notamment celles de la protection ou de la responsabilité des consommateurs. L'interprétation des principes ne devrait pas attribuer la responsabilité aux utilisateurs finals. Des lois ou d'autres mesures pourraient être adoptées afin de répondre aux besoins des utilisateurs finals, particulièrement en ce qui concerne les risques et les responsabilités assumés par les personnes physiques participant aux processus d'authentification.

Le milieu de l'authentification est dynamique et les technologies en cause continueront d'évoluer. Bien que les principes aient été définis de sorte à inclure des développements prévisibles, ces derniers sont sujets à révision puisqu'il faudra tenir compte des percées technologiques importantes, des changements dans les caractéristiques du marché et des nouveautés internationales. Les commentaires et les points de vue sur les principes sont toujours les bienvenus et devraient être adressés à :

Richard Simpson
Directeur général
Direction générale sur le
commerce électronique
Industrie Canada
300, rue Slater, pièce D2090
Ottawa (Ontario) K1A 0C8

Les commentaires peuvent aussi être envoyés par télécopieur au (613) 941-0178 ou par courriel à **authen@ic.gc.ca**.

Les principes seront examinés au moins tous les cinq ans ou plus souvent au besoin. Le Groupe de travail sur les principes d'authentification est chargé de l'examen et de la révision périodiques des principes. La composition de ce Groupe sera évaluée et modifiée s'il y a lieu à mesure que le contexte d'authentification évoluera.

AU SUJET DES PRINCIPES

CONCEPTS ET TERMINOLOGIE

Les principes qui suivent ont pour objet l'authentification des communications électroniques dans son sens large. Les concepts et les termes employés dans le présent document se rapportent donc à toutes les parties prenantes, les mesures et les techniques incluant tous les aspects de l'authentification, que ce soit du point de vue technique, juridique ou commercial. Chaque concept ou terme se rapporte aux autres; aucun d'eux ne devrait être considéré isolément.

Fonctions

Aux fins des présents principes, on considère que le processus d'authentification comporte six fonctions. Leur importance relative dépend du but et de la structure du processus d'authentification.

ADMINISTRATION DE L'AUTHENTIFICATION. Administrer la mesure ou les mesures conçues pour confirmer les attributs d'une partie prenante et la mesure ou les mesures conçues pour appuyer la crédibilité d'une partie prenante qui soutient posséder ces attributs et, par conséquent, être authentifiée.

SPÉCIFICATION. Établir ou choisir un processus d'authentification et un mécanisme d'exécution.

UTILISATION FINALE. Envoyer ou recevoir une communication électronique authentifiée et se fier à l'authentification des attributs.

ÉLABORATION DE NORMES. Établir des normes qui appuient l'élaboration continue de processus conçus pour faciliter l'authentification des communications électroniques.

ÉVALUATION DE LA CONFORMITÉ. Observer les pratiques liées à l'authentification et en faire des évaluations éclairées afin de s'assurer que les politiques, les procédures et les normes appropriées sont respectées.

PRESTATION D'INFRASTRUCTURE. Fournir la capacité technique qui permet l'authentification, y compris les fonctions permettant d'authentifier l'identité ou l'intégrité des communications électroniques.

Définitions

Les définitions existantes, particulièrement celles établies par des groupes de normalisation internationale comme l'Organisation internationale de normalisation (ISO), ont été considérées par le Groupe de travail sur les principes d'authentification lors de l'établissement des principes. Toutefois, en raison de la portée générale des principes, ces définitions ne correspondaient nécessairement pas à l'emploi qu'on en fait dans des milieux particuliers.[2]

AUTHENTIFICATION. Processus qui atteste des attributs des parties prenantes à une communication électronique ou de l'intégrité de la communication.

ATTRIBUTS. Information concernant l'identité, les privilèges ou les droits d'une partie prenante ou d'une autre entité authentifiée.

PARTIE PRENANTE. Personne ou organisation qui participe à un processus d'authentification, que ce soit directement ou par l'intermédiaire d'une autre entité authentifiée, comme un service de transmission de données ou un objet de données, un périphérique ou un programme logiciel.

COMMUNICATION ÉLECTRONIQUE. Transmission, message ou transaction électronique.

INTÉGRITÉ. Assurance que l'information contenue dans une communication électronique n'a pas été modifiée ou corrompue durant le processus de communication.

L'authentification est censé promouvoir la confiance dans la communication électronique. Les parties prenantes à une communication électronique ont l'assurance que les autres parties prenantes ont été authentifiées par des méthodes technologiques et qu'elles peuvent se fier à ces autres parties prenantes, ainsi qu'à l'intégrité de la communication, dans la mesure précisée par l'authentificateur (l'autorité dési-

2. Par exemple, la définition d'*authentification* englobe le concept d'« authentification de message », qui correspond aux procédés utilisés pour assurer l'intégrité des messages. De plus, le terme *non-répudiation* n'a pas été défini en relation avec les principes. Ce terme est couramment employé pour décrire une norme technique à laquelle le processus d'authentification doit répondre. Ce terme est toutefois trompeur dans un contexte général, car il laisse faussement entendre une conclusion de droit.

gnée qui confirme les attributs d'une partie prenante ou d'une entité et qui en atteste ensuite auprès des autres parties prenantes à la communication électronique). Les parties prenantes se fient à l'authentification d'une communication électronique dans la mesure où elles peuvent évaluer la fiabilité de l'authentification. Les méthodes et les spécifications technologiques utilisées pour l'authentification sont souvent basées sur des techniques cryptographiques.

L'authentification comme telle dépend de certaines activités préalables qui autorisent les parties prenantes, sur présentation de certains attributs donnés, à prendre part à une communication électronique authentifiée. Les attributs d'une partie prenante peuvent avoir rapport avec l'identité d'une personne. Il se peut aussi que les attributs requis concernent les droits ou les privilèges qu'a cette personne de prendre part à une communication électronique. Dans le dernier cas, il se peut que l'identité personnelle d'un partie prenante n'ait pas à être communiquée aux autres parties prenantes.

Les processus d'authentification attestent souvent des attributs d'entités non humaines. Par exemple, une organisation participant à un processus d'authentification peut choisir d'authentifier un serveur. Le cas échéant, les attributs du serveur peuvent avoir trait aux privilèges qui lui ont été assignés de communiquer avec d'autres serveurs ou clients du système.

L'autorisation relève d'une autorité désignée. Il existe de nombreux modèles pour octroyer une telle autorisation. Par exemple, pour être autorisé, un simple échange d'information peut ne nécessiter que la présentation d'un nom d'utilisateur et d'un mot de passe. Un système électronique établi pour communiquer des renseignements hautement confidentiels et privés peut, par ailleurs, nécessiter la présentation en personne d'une ou deux pièces d'identité fiables ainsi que la présentation de caractéristiques personnelles distinctes, comme les empreintes digitales. Un autre modèle peut désigner un employeur comme autorité : c'est alors ce dernier qui autorise un groupe

d'employés à échanger, en son nom, des communications électroniques d'après les fonctions du poste de chacun.

PORTÉE ET NATURE DES PRINCIPES

Ces principes se rapportent à l'authentification des communications électroniques dans son sens large.

Les principes sont censés s'appliquer aux processus d'authentification utilisés en rapport avec les communications électroniques entre des entreprises ou des administrations publiques et d'autres organisations, entre des organisations et des personnes physiques (les consommateurs et les citoyens), et entre des personnes physiques.

Il peut exister toutes sortes de relations entre les authentificateurs et les utilisateurs finals, et entre les utilisateurs finals. Nombreuses sont ces relations qui sont régies par des ententes. Les principes sont censés orienter l'élaboration de ces ententes et s'appliquer à la gamme complète de ces relations.

Les parties à des contrats négociés sont habituellement les mieux placées pour déterminer les modalités qui conviennent à leurs besoins particuliers. Toutefois, les principes revêtent une importance particulière dans les situations où une partie peut ne pas avoir la possibilité de négocier les modalités de son interaction avec l'autre partie (ou les autres parties) à la transaction.

Les principes devraient être considérés et appliqués comme s'ils formaient un tout.

Les dispositions des divers principes sont interreliées et interdépendantes; les principes ne peuvent pas atteindre leurs buts s'ils sont mis en œuvre sélectivement, quoiqu'ils peuvent ne pas tous s'appliquer dans tous les cas. Les personnes chargées d'appliquer les principes pour définir ou mettre en œuvre les processus d'authentification sont encouragées à dépasser les points de repère que les principes établissent et à les élargir en vue de répondre aux exigences de leur application ou de leur contexte de sécurité particulier.

Les principes sont de nature très générale et ils sont neutres sur le plan technologique.

Les Canadiens peuvent choisir parmi une variété de technologies pour authentifier leurs communications électroniques, selon la nature de la communication particulière et les exigences des parties prenantes.

La mise en œuvre des processus d'authentification varie aussi en fonction des objectifs commerciaux ou légaux à atteindre ainsi que des caractéristiques de l'environnement dans lequel la communication électronique se fera, comme les besoins en matière de sécurité et de protection des renseignements personnels et les autres obligations législatives ou réglementaires. Ces facteurs définissent la fonctionnalité requise d'un processus d'authentification et, dans certains cas, ils définiront même le type d'authentification utilisé.

Les principes sont conçus de manière à favoriser un marché juste et concurrentiel qui fonctionne bien pour les produits et les services d'authentification.

Les processus d'authentification devraient être efficaces, efficients, fiables et faciles à appliquer; ils devraient également respecter les intérêts des personnes physiques et morales. Chaque fois que la chose est possible, les principes laissent place au choix : choix de la technologie, choix des services, des solutions et du degré de confiance par les utilisateurs finals et choix des outils utilisés pour assurer la conformité.

Les principes mettent l'accent sur la proportionnalité.

Le niveau de responsabilité et de risque assumé par chaque partie prenante au processus d'authentification devrait être raisonnablement proportionnel au niveau de connaissance que celle-ci devrait posséder et au niveau de contrôle qu'elle devrait exercer ainsi qu'à la

nature et à la valeur de la communication électronique même. Étant donné que les parties prenantes peuvent accomplir des fonctions multiples, qui peuvent être combinées différemment, le niveau de risque et de responsabilité assumé par une partie prenante peut varier selon ces fonctions.

Les principes mettent l'accent sur la protection des renseignements personnels.

Les principes reconnaissent que le cadre juridique qui existe au Canada pour la protection des renseignements personnels évolue et ils tiennent compte de la façon dont les normes de protection des renseignements personnels s'appliquent à l'authentification. Les principes visent la jonction entre les pratiques liées au respect de la vie privée et les pratiques liées à l'amélioration de la sécurité. L'importance de la protection des renseignements personnels pour les Canadiens oblige les responsables de la conception et de la mise en œuvre des mesures d'authentification électronique à voir comment leurs systèmes peuvent le mieux respecter la protection des renseignements personnels à chaque étape du processus.

Les principes ont été élaborés afin d'assurer la compatibilité avec les innovations internationales dans le domaine de l'authentification.

Le Canada est engagé à continuer de participer aux différents forums internationaux qui traitent de la nécessité de créer des cadres mondiaux pour l'authentification. Cette participation fait en sorte que l'approche du Canada reste alignée sur celle des autres pays, ce qui permet à l'industrie canadienne d'être concurrentielle sur le marché international.

PRINCIPES

PRINCIPE 1 : RESPONSABILITÉS DES PARTIES PRENANTES

Les parties prenantes à un processus d'authentification devraient être conscientes des fonctions qu'elles accomplissent et des responsabilités liées à ces fonctions. Les responsabilités des parties prenantes sont proportionnelles au niveau de connaissance que celles-ci devraient posséder et au niveau de contrôle qu'elles devraient exercer.

Toutes les parties prenantes devraient agir prudemment et prendre des mesures raisonnables pour s'informer de la nature du processus d'authentification, notamment des exigences et des limites du processus, pour protéger l'information liée au processus et pour gérer les risques auxquels elles s'exposent (voir le principe 2).

Les responsabilités particulières des parties prenantes se rattachent à la fonction ou aux fonctions qu'elles exercent, dont les suivantes :

Administration de l'authentification

Il incombe à l'administrateur d'appliquer des mesures appropriées et éprouvées de sorte que les autres parties prenantes puissent avoir confiance dans la crédibilité des attributs revendiqués. Lorsque l'administrateur délègue une partie de la fonction d'administration à un tiers, il lui appartient de s'assurer que le tiers applique aussi des processus appropriés et éprouvés.

Spécification

La partie prenante responsable de la spécification est chargée de choisir un système, comme une infrastructure ou un processus d'authentification, qui répond aux exigences de protection des renseignements personnels et de sécurité et aux autres exigences politiques et juridiques liées à une communication électronique. Cela peut comprendre le mécanisme par lequel on vérifie l'autorisation d'une partie prenante de prendre part à une communication électronique et l'intégrité de la communication comme telle.

Utilisation finale

La responsabilité qu'ont les utilisateurs finals de s'informer du processus d'authentification est limitée par la mesure dans laquelle une information claire et évidente leur est divulguée (voir le principe 5). La responsabilité qu'ont les utilisateurs finals de protéger l'information concernant le processus

d'authentification peut être limitée par des obligations juridiques ou contractuelles. Tel est le cas lorsque celles-ci obligent les utilisateurs à divulguer de l'information se rapportant au processus qu'ils utilisent pour déterminer la fiabilité des communications électroniques.

Élaboration de normes

Les parties responsables de l'élaboration de normes sont chargées de veiller à ce que les normes soient solides, extensibles et adaptables afin d'encourager l'uniformité dans la mise en œuvre de l'authentification. Cette responsabilité englobe l'incorporation d'une vaste gamme de points de vue et de pratiques exemplaires dans les normes proposées, ce qui permet de voir à ce qu'elles soient pertinentes, actuelles et continuellement applicables. Une élaboration de normes prudente tient compte des technologies et des pratiques internationales existantes et émergentes.

Évaluation de la conformité

Il incombe aux responsables de l'évaluation de la conformité de maintenir et d'appliquer des connaissances et des pratiques professionnelles et actuelles afin de pouvoir fournir une évaluation raisonnée et éclairée des processus d'authentification.

Prestation d'infrastructure

Les prestataires d'infrastructure sont chargés de respecter les pratiques exemplaires et les normes pour mettre en œuvre et appuyer l'infrastructure qui permet l'authentification.

PRINCIPE 2 : GESTION DU RISQUE

Les risques liés aux processus d'authentification des communications électroniques devraient être déterminés, évalués et gérés d'une manière raisonnable, juste et efficace.

Les responsabilités des parties prenantes en matière de gestion des risques sont proportionnelles au niveau de connaissance que celles-ci devraient posséder et au niveau de contrôle qu'elles devraient exercer. On reconnaît que la capacité des parties prenantes de déterminer, d'évaluer et de gérer les risques varie considérablement et qu'on ne peut pas raisonnablement attendre de certaines parties prenantes (par exemple les consommateurs et les petites entreprises) qu'elles déterminent, évaluent et gèrent les risques dans la même mesure que les parties prenantes qui ont accès à des ressources plus importantes ou qui définissent les relations de travail.

Détermination

Les risques devraient être déterminés dans la mesure du possible. Les risques peuvent être financiers, incluant les dommages immédiats, directs et indirects issus d'une exécution défectueuse ou d'un retard d'exécution de la communication; ils peuvent aussi se rapporter, entre autres, à la perte de confidentialité ou de renseignements personnels, à des dommages à la réputation et au vol d'identité.

Évaluation

La gravité et l'incidence possible des risques devraient être évaluées. Lorsqu'on évalue les risques, il faut prêter une attention spéciale aux circonstances où l'on fait confiance au processus d'authentification; en outre, il peut être utile de tenir compte des responsabilités liées à chacune des six fonctions (voir le principe 1).

Gestion

Les risques devraient être gérés jusqu'à hauteur de la plus grande efficience économique, c'est-à-dire qu'ils doivent être assumés, évités, réaffectés ou atténués. Le risque est efficient sur le plan économique lorsque le risque résiduel qu'une partie prenante assume après avoir géré les risques avec prudence n'est pas plus grand que les avantages qu'elle tire de sa participation.

Rôle des contrats

Les contrats peuvent être utilisés pour encadrer la participation de chaque partie prenante. Les contrats devraient indiquer clairement les risques assumés par chaque partie et répartir les risques de manière raisonnable, juste et efficiente. Dans le cas des contrats qui ne sont pas négociés librement entre parties égales[3], il peut être nécessaire de prendre des mesures pour protéger les intérêts des parties les plus faibles.[4]

Processus de décision

Peu importe les moyens utilisés pour attribuer les risques, l'attribution devrait être raisonnable et juste et tenir compte de la capacité des parties prenantes de gérer les risques ou d'absorber les pertes. Elle devrait aussi inciter les parties chargées de l'élaboration et de la mise en œuvre des processus d'authentification à voir à ce que leurs produits et leurs services soient sûrs et fiables.

3 Un exemple d'un tel cas sont les contrats qui imposent la durée des services aux utilisateurs.

4 Les mesures en ce sens peuvent être prises au niveau du secteur d'activité et se traduire par l'inclusion de dispositions dans les codes ou au niveau gouvernemental et se traduire par l'adoption de politiques ou de lois.

PRINCIPE 3 : SÉCURITÉ

Toutes les parties prenantes à un processus d'authentification devraient être responsables et comptables de la sécurité en proportion des rôles qu'elles ont joués dans ce processus. Toutes les parties prenantes sont chargées de contribuer à atténuer les risques grâce à de saines pratiques en matière de sécurité. Toutefois, il appartient principalement aux prestataires d'infrastructure et aux intervenants dans l'administration de l'authentification de concevoir et d'offrir des systèmes basés sur des politiques et des procédures qui tiennent compte des lois, des règlements, des politiques, des normes industrielles et du contexte socio-culturel pertinents.[5]

La sécurité de l'information a pour objet d'atténuer les risques inhérents au partage d'information par voie électronique. Les prestataires d'infrastructure et les intervenants dans la spécification et l'administration des processus d'authentification prennent souvent l'initiative dans la conception et la mise en œuvre des mécanismes de sécurité et ils ont donc intérêt à sensibiliser davantage les autres parties prenantes en les renseignant sur ces mécanismes et sur le rôle qu'elles ont à jouer dans leur maintien (par exemple, choix et protection des mots de passe des utilisateurs). Les mécanismes de sécurité devraient se conformer aux normes généralement reconnues.

Protection, détection et réaction

S'il y a lieu, toutes les parties prenantes devraient être mises au courant et, en tout temps, être conscientes des risques pour la sécurité, des menaces connues et des vulnérabilités ainsi que des mesures de protection existantes. Dans un processus d'authentification, un incident de sécurité qui touche une seule partie prenante peut avoir des répercussions pour toutes les parties prenantes. Les parties prenantes devraient donc en tout temps agir de

5. Le principe de la sécurité reconnaît et adopte les *Lignes directrices de l'OCDE* [Organisation de coopération et de développement économiques] *régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité* (voir page 24). Le texte intégral des *Lignes directrices* se trouve en ligne à l'adresse suivante : **www.oecd.org/dataoecd/16/22/15582260.pdf**.

manière à prévenir de tels incidents et elles devraient être prêtes à répondre de façon appropriée et capables de le faire. Les parties prenantes devraient échanger des informations au sujet des menaces, des vulnérabilités et des risques connus, car c'est une mesure de prévention efficace qui permet d'accroître la vigilance au niveau de la détection et d'assurer une réponse opportune. Les mesures de sécurité de l'information efficaces devraient être proportionnelles au risque pour l'information et devraient respecter les droits des parties prenantes, conformément aux principes démocratiques d'une société ouverte.

Les technologies de l'information évoluent rapidement. Par conséquent, une saine gestion de la sécurité consisterait à faire en sorte que toutes les parties prenantes soient informées de manière fiable des menaces nouvelles et existantes et du rôle que les parties prenantes devraient jouer pour prévenir, détecter et régler les incidents.

Examen et évaluation

Il est essentiel d'examiner et d'évaluer continuellement les programmes de sécurité afin d'en assurer l'efficacité permanente. Les responsables de l'établissement des processus d'authentification et les prestataires d'infrastructure en particulier, de concert avec les autres parties prenantes au processus d'authentification, devraient vérifier et prouver qu'ils adhèrent à de saines pratiques de gestion de la sécurité, chacun en proportion du rôle qu'il joue. Une personne indépendante du processus d'authentification devrait examiner périodiquement les pratiques de sécurité associées au processus. Un tel examen devrait faire partie intégrante de l'accréditation et de la certification au regard des normes généralement reconnues.

PRINCIPE 4 :
PROTECTION DES RENSEIGNEMENTS PERSONNELS

Les organisations engagées dans la conception ou l'exécution des processus d'authentification devraient se conformer aux normes de protection des données énoncées dans les codes de pratique (codes en matière de protection des renseignements personnels) en plus de se conformer aux lois et à la jurisprudence (lois en matière de protection des renseignements personnels)[6] applicables. En particulier, la collecte, l'utilisation et la divulgation de renseignements personnels[7] devraient être réduites au minimum dans le contexte de l'authentification.

L'authentification fondée sur l'identité peut entrer en conflit avec les questions de protection des renseignements personnels. Par exemple, une authentification plus poussée peut nécessiter la collecte et la comparaison d'une plus grande quantité de renseignements personnels. Toutefois, il est essentiel à la sécurité et à la protection des renseignements personnels de réduire au minimum la collecte, l'utilisation et la divulgation de renseignements personnels dans le contexte de l'authentification. Des mesures de protection des renseignements personnels peuvent en fait contribuer à la sécurité des processus d'authentification.

Administration de l'authentification

L'administration de l'authentification devrait faire intervenir la collecte de renseignements personnels seulement lorsqu'elle est nécessaire. Les renseignements personnels recueillis ne devraient être utilisés qu'aux fins d'authentification. L'authentification d'une entreprise devrait focaliser sur les attributs de l'entreprise plutôt que sur les attributs personnels des employés individuels.

---

6 Les lois générales de protection des renseignements personnels dans le secteur privé qui sont actuellement en vigueur incluent la *Loi sur la protection des renseignements personnels et les documents électroniques* (loi fédérale) et les lois adoptées par l'Alberta, la Colombie-Britannique et le Québec. Les autres provinces ainsi que les territoires peuvent choisir d'adopter des lois générales de protection des renseignements personnels. Des lois fédérales, provinciales et territoriales en matière de protection des renseignements personnels qui s'appliquent au secteur public et des lois de protection des renseignements personnels propres à un secteur peuvent aussi s'appliquer. Le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation, (CAN/CSA-Q830-96), a été incorporé dans la loi fédérale intitulée *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, chap. 5, à titre d'annexe 1. Le code a été élaboré par un groupe de travail multipartite et adopté par le Conseil canadien des normes à titre de norme nationale en 1996. Beaucoup de codes de pratiques industriels traitent aussi de la protection des renseignements personnels.

7 Conformément à la définition de la *Loi sur la protection des renseignements personnels et les documents électroniques* : « tout renseignement concernant un individu identifiable ».

Si la collecte de renseignements personnels est nécessaire, elle doit être réduite au minimum. L'utilisation ou la divulgation de renseignements personnels devrait également être réduite au minimum. Les renseignements personnels ne devraient être recueillis, utilisés ou divulgués qu'avec le consentement éclairé de la personne physique.

Les renseignements personnels ne devraient être conservés qu'aux fins d'authentification.

Spécification et prestation d'infrastructure

Les processus d'authentification doivent être conçus de manière à exiger que le moins possible de renseignements personnels soient recueillis, utilisés et divulgués. La conception des processus devrait tenir compte des droits d'accès des parties prenantes et de l'obligation qu'ont les organisations de communiquer de l'information au sujet de leurs politiques en matière de protection des renseignements personnels. Les organisations qui utilisent des processus d'authentification conçus par d'autres sont chargées de faire en sorte que ces processus protègent les renseignements personnels.

Utilisation finale

Les utilisateurs finals des processus et des services d'authentification devraient prendre des mesures raisonnables pour s'assurer que les renseignements personnels placés sous leur contrôle sont protégés contre la collecte, l'utilisation ou la divulgation non autorisée.

Élaboration de normes

Les normes d'authentification devraient être élaborées en pleine conformité avec les principes concernant la protection des renseignements personnels qui sont énoncés dans les lois et les codes sur la protection des renseignements personnels. La protection des renseignements personnels devrait être explicitement enchâssée dans les normes d'authentification. Les responsables de l'élaboration des normes devraient tenir compte de la concordance entre les mesures qui contribuent à la protection des renseignements personnels et celles qui sont conçues pour assurer la sécurité des processus d'authentification.

Évaluation de la conformité

L'évaluation de la conformité devrait notamment déterminer si l'organisation en question se conforme aux principes de protection des renseignements personnels énoncés dans les lois et les codes. Les évaluateurs de la conformité devraient protéger la confidentialité des renseignements personnels dont ils prennent connaissance dans le contexte de leurs évaluations, conformément aux lois et aux codes sur la protection des renseignements personnels.

PRINCIPE 5 :
OBLIGATIONS D'INFORMATION

Les parties prenantes qui offrent des services d'authentification devraient divulguer des informations aux autres parties prenantes afin de faire en sorte que toutes les parties prenantes soient conscientes des risques et des responsabilités inhérents à leur participation.

L'information qui est divulguée concernant les services d'authentification devrait inclure les politiques, les pratiques et les procédures et indiquer si les services sont examinés ou vérifiés régulièrement. Une divulgation appropriée exige que l'information soit suffisamment détaillée pour l'objectif visé, qu'elle soit formulée en langage simple et qu'elle soit évidente. Les trois facteurs auront une incidence sur la connaissance de l'information divulguée que les autres parties prenantes devraient raisonnablement posséder.

Étendue et nature de la divulgation

L'information divulguée *ne* devrait *pas* inclure les informations liées à la sécurité qui, si elles étaient divulguées, introduiraient des vulnérabilités et augmenteraient le risque. Toutefois, la quantité et la nature des informations divulguées devraient permettre aux parties prenantes de comprendre leurs responsabilités et de prendre des décisions éclairées en matière de gestion du risque, pour ce qui est de la confiance à accorder à l'authentification. La portée et la nature de l'information peuvent varier selon que l'utilisateur final est une personne physique ou une organisation.

Notification

Les parties prenantes devraient être informées de l'accessibilité d'une telle information et des changements qui y sont apportés. Il se peut qu'une preuve de la notification soit exigée, selon la nature du processus d'authentification et des applications connexes.

Lien aux autres principes

Les parties prenantes qui offrent des services d'authentification devraient divulguer leur politique et leurs pratiques en matière de collecte de renseignements personnels. Le principe 4 de la protection des renseignements traite plus en profondeur des renseignements personnels et de leur divulgation.

Les obligations d'information doivent du même coup être considérées de concert avec le principe 1 (responsabilités des parties prenantes) et le principe 2 (gestion du risque).

PRINCIPE 6 : TRAITEMENT DES PLAINTES

Les organisations qui mettent en œuvre un processus d'authentification devraient élaborer une méthode de traitement des plaintes permettant aux parties prenantes de répondre à ces plaintes de façon efficace et efficiente, et de régler les problèmes d'inobservation de façon appropriée.

Les processus de traitement des plaintes devraient refléter les éléments suivants.

Visibilité

L'information sur les modalités de dépôt des plaintes devrait être communiquée à toutes les parties prenantes et à leur personnel et aux autres parties intéressées et devrait inclure des renseignements complets sur le processus de traitement des plaintes.

Accessibilité

Le processus de traitement des plaintes devrait être facilement accessible à toutes les parties prenantes et l'organisation doit faire en sorte qu'il soit facile d'obtenir des renseignements sur les détails du règlement des différends. Le processus et l'information à l'appui devraient être faciles à comprendre et à utiliser par les personnes physiques faisant des plaintes. Ils devraient être expliqués en langage simple et être accessibles dans les langues des produits et des services offerts à l'origine.

Rapidité de réaction

Les plaintes devraient faire l'objet d'une étude rapide et minutieuse. Elles devraient être examinées du point de vue de la sécurité et réglées en priorité, selon les répercussions négatives qu'elles pourraient avoir sur les parties prenantes en cause ou sur la mise en œuvre de l'authentification dans l'ensemble.

Équité et objectivité

Chaque plainte devrait être réglée de manière objective grâce au processus de traitement des plaintes et le règlement devrait être équitable pour le plaignant et pour la partie prenante visée par la plainte.

Frais

L'accès au processus de traitement des plaintes ne devrait rien coûter au plaignant.

Confidentialité et protection des renseignements personnels

Les renseignements personnels sur les plaignants devraient être accessibles seulement aux points de l'organisation qui traitent la plainte et ils doivent être activement protégés contre toute divulgation à moins que le plaignant consente expressément à la divulgation.

Reddition de comptes

Les organisations devraient s'assurer qu'une personne physique désignée ou qu'une unité identifiable de l'organisation soit responsable de la consignation systématique des plaintes et de leur règlement, et qu'elle rende compte des actions et des décisions de l'organisation relativement au traitement des plaintes.

Amélioration continue

L'amélioration continue de la qualité des produits et services est facilitée par le processus de traitement des plaintes qui est basé sur les commentaires des clients et d'autres parties. Le processus même de traitement des plaintes devrait être surveillé en permanence et examiné et évalué à la lumière des commentaires.

Plaintes non réglées

Dans les cas où les plaintes ne peuvent pas être réglées à l'interne, les organisations devraient être prêtes à utiliser les processus de règlement des plaintes de tiers, à la demande du plaignant, y compris les processus administrés par des tiers du secteur privé. Toutefois, les plaignants devraient continuer à avoir accès au système de justice.

INFORMATIONS SUPPLÉMENTAIRES ET RÉFÉRENCES

INFORMATIONS SUPPLÉMENTAIRES

Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information

1. Sensibilisation

Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.

2. Responsabilité

Les parties prenantes sont responsables de la sécurité des systèmes et réseaux d'information.

3. Réaction

Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.

4. Éthique

Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.

5. Démocratie

La sécurité des systèmes et réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.

6. Évaluation des risques

Les parties prenantes doivent procéder à des évaluations des risques.

7. Conception et mise en œuvre de la sécurité

Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.

8. Gestion de la sécurité

Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.

9. Réévaluation

Les parties prenantes doivent examiner et réévaluer la sécurité des systèmes et réseaux d'information et introduire les modifications appropriées dans leurs politiques, pratiques, mesures et procédures de sécurité.

RÉFÉRENCES

Voir **http://strategis.ic.gc.ca/authen-fr** pour obtenir une bibliographie générale renfermant des ouvrages de référence nationaux ou internationaux, ainsi que les documents sources spécifiques de chaque principe.